线性扫频干扰检测算法及抗干扰方法研究 *

韩 晨[1]，牛英滔[2]，夏 志[1]，逄天洋[1]

(1. 陆军工程大学，南京 210000; 2. 南京电讯技术研究所，南京 210007)

摘 要：线性扫频干扰是战场中常用的干扰样式之一，对其进行及时检测并做出高效抗干扰决策具有重要意义。提出一种考虑虚警概率和漏检概率指标的低复杂度线性扫频干扰检测算法，并对算法性能进行了理论分析，为实际通信系统判断受扰情况提供判断依据；然后，提出一种基于 Q 学习的抗扫频干扰算法，可在无线通信系统遭遇扫频干扰时，自主选择最佳的通信信道和最长驻留时间。最后仿真结果表明所提检测算法可有效检测出线性扫频干扰信号，以较低复杂度得到与理论分析结果相近的检测性能。所提抗扫频干扰学习算法可在干扰环境中自主选择通信信道，高效规避扫频干扰，实现持续可靠的信息传输。

关键词：线性扫频干扰；通信抗干扰；漏检概率；虚警概率；Q 学习；信道选择

中图分类号：TN918.91 doi: 10.19734/j.issn.1001-3695.2018.05.0449

Detection algorithm and anti-jamming method for linear sweeping jamming with low complexity

Han Chen[1], Niu Yingtao[2], Xia Zhi[1], Pang Tianyang[1]

(1 *Army Engineering University*, *Nanjing* 210000, *China*; 2 *Nanjing Telecommunication Technology Institute*, *Nanjing* 210007, *China*)

Abstract: The linear sweeping jamming is one of the common jamming patterns in the battlefield. It is of great significance to detect the sweeping jamming and make effective anti-jamming decision. In this paper, the authors proposed a detection algorithm for sweeping jamming with low complexity under the constraint of the probability of false alarm and missed detection, and theoretically analyzed the performance of the detection algorithm to provide the basis for judging the disturbance of the actual communication system. Then, the authors proposed an anti-jamming learning algorithm based on Q-Learning, which can be used to autonomously select the best communication channel and the maximal reliable transmission time when the wireless communication system is threatened by sweeping jamming. Finally, the simulation results show that the proposed detection algorithm can effectively detect the linear sweeping jamming, and the detection performance is basically consistent with the theoretical analysis results with low complexity. The anti-jamming learning algorithm can adaptively determine the optimal communication channel, and effectively avoid the sweeping jamming to realize the reliable information transmission.

Key words: linear sweeping jamming; communication anti-jamming; probability of missed detection; probability of false alarm; Q-learning; channel selection

0 引言

军事无线通信已成为决定现代战争胜负的关键因素之一，其可靠性和有效性将直接决定战场信息的共享程度[1]。敌方的恶意干扰是影响无线通信可靠性与有效性的主要因素之一，而线性扫频干扰具有产生简单、干扰带宽大、干扰效率高等优势，已成为敌方常用的干扰样式之一，所以对线性扫频干扰进行及时有效的检测具有重要意义[2]。

目前对线性扫频干扰的检测已经有了一些成熟的分析方法和思路。Wigner-Ville 分布对线性扫频干扰的检测而言，具有良好的视频聚集性，但当干扰数目增加时，易受交叉项的影响[3]。文献[4~6]提出与 Hough 变换结合的 Wigner-Houg 变换算法，进一步改善了检测性能。文献[7]提出基于似然梯度的隐马尔可夫模型识别算法，并对模型参数进行实时估计，解决了扩频通信

收稿日期：2018-05-15；**修回日期：**2018-07-02 **基金项目：**江苏省自然科学基金资助项目（BK20151450）

作者简介：韩晨（1993-），男，山东滨州人，硕士研究生，主要研究方向为认知无线电、无线通信抗干扰（chenhan2017lgd@163.com）；牛英滔（1978-），男，山东泰安人，高级工程师，博士，主要研究方向为认知无线电、无线通信抗干扰；夏志（1993-），男，江苏涟水人，硕士研究生，主要研究方向为认知无线电、无线通信抗干扰；逄天洋（1993-），男，黑龙江哈尔滨人，硕士研究生，主要研究方向为认知无线电、无线通信抗干扰.

中扫频干扰的抑制问题[8]。文献[9]则利用分数阶傅里叶变换方法在分数阶域对扫频信号进行干扰检测。这些文献对于扫频信号的检测及其抑制都做出了有益的探索[10]。但是，已有算法还存在复杂度高、主要检测弱扫频信号、缺乏对检测性能的理论分析等问题，难以满足军事无线通信系统对于扫频干扰的感知要求。

以Q学习为代表的强化学习技术在无线通信中已经得到广泛应用。文献[11]研究分布式动态频谱接入网络中的频谱和功率分配问题，首先通过 Q 学习解决频谱分配问题，然后将功率分配视为最优化问题，以减少计算复杂度、增强实时性。文献[12]提出基于 Q 学习的实时路由选择算法，解决在移动自组织网络中，由于节点的可移动性带来的路由选择不稳定问题。文献[13]在抗干扰博弈框架下，采用最小最大 Q 学习解决认知干扰威胁下的频谱分配问题。已有文献中，应用强化学习技术进行抗扫频干扰决策的研究还较少。对于遭受干扰攻击的无线通信系统而言，可引入强化学习技术，通过对干扰的感知和学习，发现干扰规律，有效预测干扰行为，使无线通信系统可以动态适应电磁环境，实现高效可靠的数据传输。

本文研究了在虚警概率、漏检概率等性能指标的约束下，对线性扫频干扰进行有效检测的问题，对检测性能进行理论推导，为实际通信系统判断受扰情况提供了理论依据。然后利用 Q 学习算法实现在扫频干扰下的可靠传输。最后基于军事无线通信需求对检测性能的理论推导及抗干扰学习算法进行仿真验证。

1　系统模型

线性扫频干扰是一种干扰信号对目标频段进行周期性线性扫描，从而有效降低目标频段内无线通信可靠性或有效性的干扰样式。本文所考虑的干扰信号为服从正态分布的窄带高斯白噪声信号，信号带宽为W_{chirp}。在一个扫描周期T内，干扰信号的中心频率从最低频f_L移动到最高频f_H，形成对目标频段的扫描式干扰。扫频干扰信号$J_{chirp}(t)$表达式为

$$J_{chirp}(t)=\text{Filter}\left[J_{w0}(t),f(t)\right] \tag{1}$$

其中：$\text{Filter}[\bullet]$表示对信号进行窄带滤波；$J_{w0}(t)$表示零均值服从正态分布的高斯白噪声信号，其方差为$N(0,\ \sigma_s^2)$；$f(t)=f_H-\frac{f_H-f_L}{T}\left(t-\left(h-1\right)\times T\right)$表示第$h\left(h=1,2\ldots\right)$个扫频周期内，窄带滤波器的瞬时中心频率。

当存在线性扫频干扰时，AWGN 信道下无线通信系统接收到的采样信号为：

$$x(n)=J_{chirp}(n)+n_0(n) \tag{2}$$

其中$x(n)$表示接收信号，$n_0(n)$表示信道中零均值的高斯白噪声，方差为σ^2。

为便于研究，对算法条件作出以下假设：

a)目标频谱由N个在频域上互不重叠的信道组成，每个信道带宽为W_{ch}，目标频谱带宽为$W=NW_{ch}$。

b)宽带检测器检测带宽为W，可检测这N个信道内的能量值，每次检测所需样点数为 2NL。扫频干扰带宽满足$W_{chirp}\le W$。

c)在整个检测过程最多检测M_1次，每次检测时长为T_d，总检测时长$M_1T_d\le T$。

d)每次检测时长T_d足够短，检测期间扫频信号可近似视为固定频率信号。

e)可靠传输时间定义为从开始通信到遭受干扰通信中断时为止，所经历的传输时间。

2　低复杂度线性扫频干扰检测算法

本章提出一种考虑虚警概率和漏检概率指标的低复杂度的线性扫频干扰检测算法，为实际通信系统判断受扰情况提供判断标准。具体算法步骤如下所示：

a）计算目标频段的功率谱。在第$m(m=1,2\ldots M_1)$个检测时刻，NP 能量检测器对目标频段使用修正周期图法进行功率谱计算。第m次检测得到的频率点f的功率谱值为

$$P_m(f)=\frac{\left|\sum_{l=0}^{2NL-1}w(l)x(l)e^{-j2\pi fl}\right|^2\Big/2NL}{\sum_{l=0}^{2NL-1}\left|w(l)\right|^2\Big/2NL}\qquad \text{m}=1,2,3\ldots M_1 \tag{3}$$

其中：$2NL$为采样点数，$x(l)$为采样值，$w(l)$为窗函数，本文选用汉明窗。

b）计算各信道中的能量值。式(3)中得到的功率谱点数为NL点，将功率谱按顺序等分为N段，每段功率谱点数为L，对应于一个信道。第m次检测第i个信道中的能量值可计算为

$$\begin{aligned}E_{m,i}&=\frac{W_{ch}}{L}\sum_{k=1}^{L}P_m(f_{[(i-1)L+k]})\\&=\frac{W}{NL}\sum_{k=1}^{L}P_m(f_{[(i-1)L+k]})\end{aligned} \tag{4}$$

c）判断N个信道中是否有信道在第m次检测中受扰。将第m次检测第i个信道的能量值$E_{m,i}$与检测门限γ比较，门限值γ由虚警概率指标P_{FA}给出：

$$\gamma=\sigma^2Q_{\chi_L^2}^{-1}\left(P_{FA}\right) \tag{5}$$

若$E_{m,i}>\gamma$则判定为m时刻i信道受到干扰，记为$I_{i,m}>0$；反之，则判为m次检测第i个信道未受到干扰，记为$I_{i,m}=0$。

d）按上述方法对目标频段检测M_1次。若第$m-1$次检测时信道i未受扰，第m次检测时该信道受扰，而$m+1$次检测时该信道的干扰消失，则判定为i信道受到动态干扰：

$$I_i=\left\{I_{m-1}=0;I_m>0;I_{m+1}=0\right\}>0 \tag{6}$$

e）根据给定的漏检概率指标P_m，计算检测信道数目的信道门限值M：

$$P_m=\sum_{k=0}^{M-1}C_N^kP_i^k\times(1-P_i)^{N-k}\qquad M=\arg\left\{P_m\right\} \tag{7}$$

其中：P_i 为单信道动态干扰检测概率。若在 M_1 次检测中，N 个信道中至少有 M 个信道受到动态干扰，则判为该频段受到动态干扰。漏检概率 P_m 定义为实际受到动态干扰，但未检测出干扰存在的概率。

f）将检测到受扰的频点分为奇偶两组，分别使用最小二乘法拟合成直线：$y_e = A_e x + B_e$,$y_o = A_o x + B_o$ 。若两条拟合直线参数的相似程度大于门限值 η ，即

$$\Delta = |A_e - A_o|^2 + |B_e - B_o|^2 < 1-\eta \tag{8}$$

即认为受到线性扫频干扰。

3　检测算法性能分析

本章对所提出的考虑虚警概率和漏检概率指标的低复杂度线性扫频干扰检测算法进行理论分析。

3.1　NP 检测器

干扰信号的检测问题可视为二元假设的选择问题，根据 NP 定理构建 NP 检测器为

$$\begin{aligned} &H_0 : x(n) = n_o(n) \\ &\quad n = 0,1...2NL-1 \\ &H_1 : x(n) = n_o(n) + J_{chirp}(n) \\ &\quad n = 0,1...2NL-1 \end{aligned} \tag{9}$$

其中：H_0 假设观测值 $x(n)$ 中只有噪声；H_1 假设观测值 $x(n)$ 中既有干扰信号又有噪声。$2NL$ 次采样相互独立，构造似然比函数 $L(x)$，若似然比超过门限值 γ'：

$$L(x) = \frac{p(x|H_1)}{p(x|H_0)} > \gamma' \tag{10}$$

NP 检测器判为 H_1 假设，判定存在干扰信号，反之判为 H_0 假设。其中 $p(x|H_1)$ 表示 H_1 假设下观测值的概率密度函数，$p(x|H_0)$ 表示 H_0 假设下观测值的概率密度函数。

3.2　干扰信号检测性能分析

根据模型假定，如式（9）所示，在 H_0 条件下，$x(n)\sim N(0,\sigma^2)$；在 H_1 条件下，$x(n)\sim N(0,\sigma^2+\sigma_s^2)$。此时对数形式的似然比函数为

$$\begin{aligned} \ln L(x) = &\frac{L}{2}\ln\left(\frac{\sigma^2}{\sigma^2+\sigma_s^2}\right) \\ &-\frac{1}{2}\left(\frac{\sigma^2}{\sigma^2+\sigma_s^2} - \frac{1}{\sigma^2}\right)\sum_{n=0}^{2NL-1} x^2[n] \end{aligned} \tag{11}$$

化简整理并将与观测值无关的常量与门限值 γ' 合并成 γ，可得检测量 $T(x)$ 为

$$T(x) = \sum_{n=0}^{2NL-1} x^2(n) > \gamma \tag{12}$$

如果 $T(x)$ 超过新门限值 γ，则判为 H_1 假设成立，判定存在干扰信号。$x(n)$ 服从高斯分布，$T(x)$ 是 $2NL$ 个独立同分布的高斯随机变量的平方和。在 H_0 条件下，T/σ^2 服从自由度为 $2NL$ 的卡方分布；在 H_1 条件下，$T/(\sigma^2+\sigma_s^2)$ 服从自由度为 $2NL$ 的卡方分布。自由度为 ν 的卡方分布用 χ_ν^2 表示。

$$\begin{aligned} &H_0 : \frac{T}{\sigma^2} \sim \chi_{2NL}^2 \\ &H_1 : \frac{T}{\sigma^2+\sigma_s^2} \sim \chi_{2NL}^2 \end{aligned} \tag{13}$$

定义 χ_ν^2 在 $[x,\infty]$ 区间内的概率积分为 $Q_{\chi_\nu^2}$：

当 $\nu=1$ 时，

$$Q_{\chi_\nu^2} = 2Q\left(\sqrt{x}\right) \tag{14}$$

$\nu>1$ 且为奇数，

$$\begin{aligned} Q_{\chi_\nu^2} = &\frac{\exp\left(-\frac{1}{2}x\right)}{\sqrt{\pi}}\sum_{k=0}^{\frac{\nu-1}{2}}\frac{(k-1)!(2x)^{k-\frac{1}{2}}}{(2k-1)!} \\ &+2Q\left(\sqrt{x}\right) \end{aligned} \tag{15}$$

$\nu>1$ 且为偶数，

$$Q_{\chi_\nu^2} = \exp\left(-\frac{1}{2}x\right)\sum_{k=0}^{\frac{\nu-1}{2}}\frac{\left(\frac{x}{2}\right)^k}{k!} \tag{16}$$

其中 $Q(x)$ 为互补累积分布函数，$\Phi(t)$ 为服从 $N(0,1)$ 分布的随机变量的概率密度函数。

3.3　单信道动态干扰检测概率

实际没有干扰却检测到干扰信号存在，这类错误用虚警概率 P_{FA} 表示为

$$\begin{aligned} P_{FA} &= P_r\{T(x) > \gamma | H_0\} \\ &= P_r\left\{\frac{T(x)}{\sigma^2} > \frac{\gamma}{\sigma^2} | H_0\right\} \\ &= Q_{\chi_L^2}\left(\frac{\gamma}{\sigma^2}\right) \end{aligned} \tag{17}$$

所以最终的检测门限值 γ 由给定的虚警概率计算得出

$$\gamma = \sigma^2 Q_{\chi_L^2}^{-1}(P_{FA}) \tag{18}$$

单信道动态干扰检测概率 P_{D1} 为实际存在干扰并且正确检测出干扰存在的概率，P_{D2} 为实际不存在干扰并且正确检测到不存在干扰的概率。P_{D1}、P_{D2} 分别为

$$\begin{aligned} P_{D1} &= P_r\{T(x) > \gamma | H_1\} \\ &= P_r\left\{\frac{T(x)}{\sigma^2+\sigma_S^2} > \frac{\gamma}{\sigma^2+\sigma_S^2} | H_1\right\} \\ &= Q_{\chi_L^2}\left(\frac{\gamma}{\sigma^2+\sigma_S^2}\right) \end{aligned} \tag{19}$$

$$\begin{aligned} P_{D2} &= P_r\{T(x) < \gamma | H_0\} \\ &= 1 - P_r\{T(x) > \gamma | H_0\} \\ &= 1 - Q_{\chi_L^2}\left(\frac{\gamma}{\sigma^2}\right) \end{aligned} \tag{20}$$

结合算法可知，信道 i 上存在动态干扰的检测概率 P_{Di} 为

$$P_{Di} = P_{D2,m-1} \times P_{D1,m} \times P_{D2,m+1} \tag{21}$$

3.4　线性扫频干扰检测性能

已知干扰存在的前提下，通信系统对动态干扰最终的漏检

概率和检测概率分别为 P_m、$P=1-P_m$。给定漏检概率指标，由式(7)可得到判决该频段是否受到动态干扰的受扰信道门限值 M。若经 M_1 次检测，N 个信道中至少有 M 个信道检出受到动态干扰即判为该频段受到动态干扰。将受扰频点线性拟合，若近似为一条直线，则判为受到线性扫频干扰。

由式(7)分析可知，信道门限值 M 设定越大，P_m 越大，P 越小，对动态干扰的检测概率越低，但是在实际检测中未知敌方干扰状态的前提下，若最终检测器判为干扰存在，则该结果的可信度也越高。

4　基于 Q 学习的抗扫频干扰算法

Q 学习算法是典型的强化学习算法，智能体应用 Q 学习算法可以根据环境的反馈信息，主动调整执行策略，实现智能体与环境的自适应交互，提高智能体对环境的适应能力。如图 1 所示，当前状态 s 下，智能体根据当前选择策略 π，选择一个动作 a 作用于未知环境，同时获得环境反馈信号 r，由此更新 Q 函数，并指导下一轮动作选择。经过不断地学习，智能体最终可以找到最优的动作选择策略 π^* [14]。

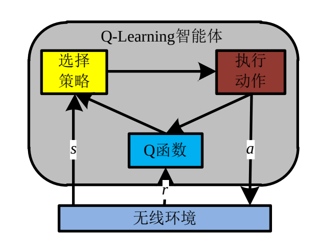


图 1　Q 学习算法

Fig .1 Q-learning algorithm

在无线通信领域中Q学习算法广泛用于解决无线通信系统与电磁环境的动态交互问题。然而，在存在恶意干扰的环境中，应用 Q 学习算法实现智能抗干扰通信的相关研究还比较少。在第 3 章检测算法的基础上，结合 Q 学习算法，本节提出一种抗扫频干扰学习算法，实现无线通信系统在扫频干扰下的智能高效的抗干扰通信。

根据检测算法结果，定义状态空间 $\mathbf{S}$，$s_t\in\mathbf{S}$：

$$\mathbf{S}=[1,2,\ldots N] \tag{22}$$

其中 s_t 为 t 时刻扫频干扰所在信道。

定义动作空间 $\mathbf{A}$，$a_t\in\mathbf{A}$：

$$\mathrm{A}=[1,2,\ldots N] \tag{23}$$

其中，a_t 表示用户在 t 时刻选择的通信信道。此时的回报函数 r_t 为

$$r_t=T_2-T_1 \tag{24}$$

其中：T_1 为开始通信时刻，T_2 为遭受干扰，通信中断时刻。用户的通信选择策略 π 定义为当前状态 s_t 下选择各种可能动作 a_t 的一种概率分布。用户的优化目标是寻找最佳的选择策略 π^*，使得用户的可靠传输时间最长。

$$\pi^*=P_r(a_t\,|\,s_t) \tag{25}$$

传统 Q 学习算法，一般采用固定 ε 贪婪模型权衡“探索”与“利用”[15]：

$$\begin{aligned} &a=random(A) && Num>\varepsilon \\ &a=\arg\max_{a'} Q(s,a') && Num\le\varepsilon \end{aligned} \tag{26}$$

其中，$\varepsilon\in(0,1)$，Num 表示生成的[0,1]之间随机数，若 $Num>\varepsilon$，则从动作集合中随机选择执行动作，“探索”更优的选择策略；若 $Num\le\varepsilon$，则“利用”已得到的 Q 表，选择可使 Q 值最大的执行动作。而对于通信抗干扰而言，通信双方在获得抗干扰决策知识后，需要建立稳定的通信行为，以满足通信需求。所以采用固定的 ε 值进行“探索”与“利用”权衡的方法，不利于学习过程的稳定收敛。故在抗干扰场景下，本文基于模拟退火模型实现“探索”与“利用”的平滑过渡，当获得完整的抗干扰决策知识后，可建立稳定的通信行为，以更好地实现智能通信抗干扰学习。

通信选择策略按下式更新：

$$\pi(a_t\,|\,s_t)=\frac{\tau^{\mathbf{Q}(s_t,a_t)/\xi}}{\tau^{\mathbf{Q}(s_t,a_t)/\xi}+\sum_{a^-}\tau^{\mathbf{Q}(s_t,a^-)/\xi}} \tag{27}$$

其中：a^- 代表除当前通信信道 a_t 外的其他信道，ξ，τ 为波尔兹曼模型的相关参数，$P_r(a_t\,|\,s_t)$ 表示在状态 s_t 下选择动作 a_t 的概率。

$$\begin{aligned} &\xi=\xi_0\tau^{(-\upsilon t)} && \xi\ge\xi_{final} \\ &\xi=\xi_{final} && \xi<\xi_{final} \end{aligned} \tag{28}$$

其中：ξ_0 与“探索”时间正相关，ξ_{final} 表示“探索”阶段的结束条件，τ、υ 影响“探索”阶段与“利用”阶段之间的过渡时间。

基于 Q 学习算法，提出抗扫频干扰算法如下所示。

a）　初始化 $\mathbf{Q}=[s,a]$ 为零矩阵，初始学习速率 α_0，学习规则中的退火初始温度 ξ_0、最终温度 ξ_{final} 及波尔兹曼参数 τ 和退火速率 υ，初始化通信选择策略 $P_r(a\,|\,s)=1/|\mathrm{A}|$，从状态集 $\mathbf{A}$ 中随机选择一个信道作为当前通信信道。

b）　在每个时隙 t，重复下面过程：

（a）　按照当前的通信策略，选择动作 a_t，计算收到的回报值 r_t

（b）时隙结束后，结合以往观测值及本次选择所得回报 r_t，按照下式更新 Q 表：

$$\mathbf{Q}_t(s_t,a_t)=(1-\alpha)\mathbf{Q}_{t-1}(s_t,a_t)+\alpha r_t \tag{29}$$

（c）根据式（27）更新通信选择策略；

（d）根据式（28）（30）更新波尔兹曼系数 ξ 及学习速率 α：

$$\alpha=\alpha_0/(\mu(s,a)\log(\mu(s,a))) \tag{30}$$

其中:α_0 表示学习起始阶段的学习步长，$\mu(s,a)$ 表示访问状态动作对 (s,a) 的次数，文献[16]已证明若满足 $\sum_{l=0}^{\infty}\alpha_l=\infty$，$\sum_{l=0}^{\infty}\alpha_l^2<\infty$，则 Q 学习算法可以收敛。

（e）判断是否达到最大迭代次数 K，若否则返回步骤 b）。

5　仿真结果

为验证所提算法的性能，运用 MATLAB 进行仿真实验。实验中设定采样频率 $Fs=20\text{MHz}$，一次检测时间 $T_d=0.5\text{ms}$，扫频信号周期 $T=0.05\text{s}$。扫频信号最低频率，最高频率及扫频干扰带宽分别为 $f_L=2\text{MHz}$，$f_H=10\text{MHz}$，$W_{chirp}=8\text{MHz}$。宽带检测器检测带宽 $W=8\text{MHz}$，可检测 $N=100$ 个信道。高斯噪声方差 $\sigma^2=0.5$，干扰噪声比 JNR 为 $-15\sim6\text{dB}$。本文采用窄带高斯噪声调幅扫频信号的方法产生扫频干扰信号。首先产生带宽为 50KHz 的窄带高斯噪声 $Gauss(n)$。然后用该噪声调幅扫频信号 $J_{chirp}(n)$，最终干扰信号 $J_{G-chirp}(n)=Gauss(n)\times J_{chirp}(n)+n_o(n)$，式中 $n_o(n)$ 为信道环境中的高斯白噪声，满足干噪比为 $-15\sim6\text{dB}$，其中 $J_{chirp}(n)=\cos\left[2\pi\left(f_H-\frac{f_H-f_L}{T}\big(n-(i-1)\times T\big)\right)n\right]$。虚警概率 P_{FA} 给定时，经上述推导可知，检测门限值 γ 由式(18)计算得出，由式(21)可计算得出单信道动态干扰检测概率 P_D。验证能量检测器的检测性能的实验结果如图 2 所示。

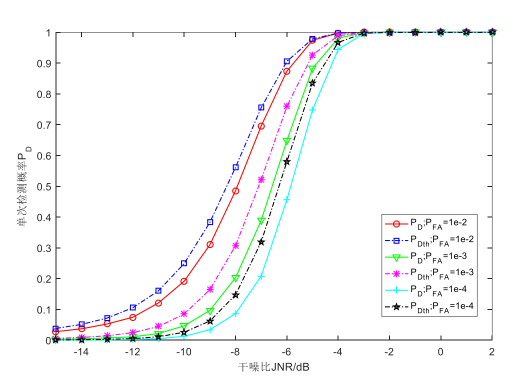


图 2　单次干扰检测概率

Fig .2 Detection probability of jamming in a single detection.

设定虚警概率 P_{FA} 分别为 10^{-2}、10^{-3}、10^{-4}，由图 2 可得，单次检测概率 P_D 与理论值 P_{Dth} 基本一致，所提检测算法以 $O(n\log n)$ 的较低复杂度实现与理论分析结果相近的检测性能。在干噪比 $JNR>-4\text{dB}$ 时，能量检测器检测性能较好，单次检测概率接近于 1。

图 3 表示，固定干噪比 $JNR=-5\text{dB}$，比较不同虚警概率约束下，系统检测概率 P 与信道门限值 M 之间的对应关系。干噪比恒定时，检测概率随着信道门限值的增大而逐渐减小，信道门限值设定越高，对动态干扰的检测概率越小，但在未知干扰状态时，检测结果的可信度越高。虚警概率指标设定越小，单次检测概率越低，设定相同信道门限值时，可得到的检测概率越低。

图 4 中固定虚警概率为 $P_{FA}=10^{-3}$，比较不同干噪比条件下，检测概率的理论值 P_{th} 与实际值 P 的仿真结果。虚警概率恒定时，检测概率、检测信道门限值一一对应，随着信道门限值增大，检测概率减小，未知干扰状态时的检测可信度增大；当干噪比 JNR 逐渐降低时，设定相同信道门限值，系统检测概率降低。实验结果表明，所以检测算法可以以较低的复杂度（$O(n\log n)$）实现与理论分析结果相近的检测性能。

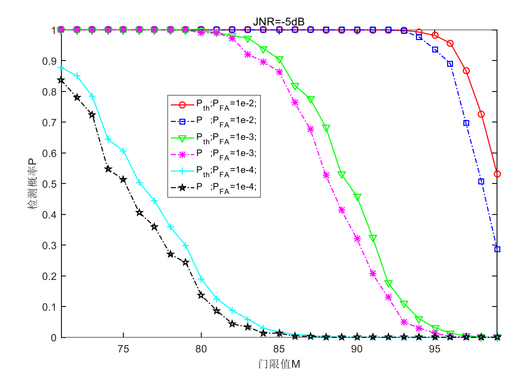


图 3　不同虚警概率条件下的检测概率

Fig .3 Detection probability under the condition of different false alarm probability.

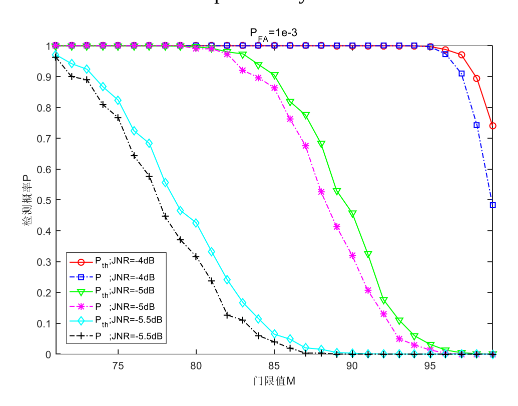


图 4　不同干噪比条件下的检测概率

Fig .4 Detection probability with different JNR.

在每个检测周期内，将受到动态干扰的信道频点分奇偶数分别进行最小二乘线性拟合，拟合曲线如图 5 中蓝色虚线所示（为便于展示抗干扰效果，此处仿真令 N=10）。图 5 中展示了两个周期内扫频干扰信号的时频干扰规律。基于检测结果，利用抗扫频干扰学习算法寻找可保证最大可靠传输时间的信道选择策略，如图 5 中红色实线所示，基于当前的干扰状态，无线通信系统自主选择的通信信道比扫频信号所在信道滞后一个信道，当扫频信号干扰最低频所在信道时，所选信道为最高频所属信道。此时，通信系统可通过自主选择通信信道，保证最大的传输驻留时间。图 6 展示了所提抗干扰算法与盲跳频抗干扰方法、及基于传统贪婪准则的 Q 学习算法（ε=0.8）抗干扰方法的平均可靠传输时间的性能比较。由图 6 可以看出，所提算法可保证更高的可靠传输时间，具有更高的抗干扰性能。

6　结束语

对线性扫频干扰信号进行及时有效的检测并提出相应的高效抗干扰策略是军事通信抗干扰方向重要的研究课题。本文提出一种对线性扫频干扰信号进行有效检测的宽带检测算法，并对该算法进行了性能分析。仿真结果表明，提出算法的检测性能可以满足给定的虚警概率和漏检概率指标，以较低复杂度实现较好的检测性能，可满足军事无线通信系统对于扫频干扰的

感知要求，同时也验证了对检测性能的基础理论分析的正确性。在检测结果的基础上，提出一种基于 Q 学习的抗扫频干扰检测算法，仿真结果表明该算法可在扫频干扰下，选择最佳信道实现持续高效的可靠传输。

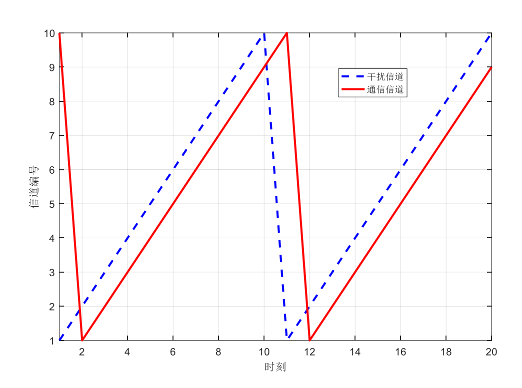


图 5　扫频干扰检测结果及信道选择策略

Fig .5 Detection results and channel selection strategies.

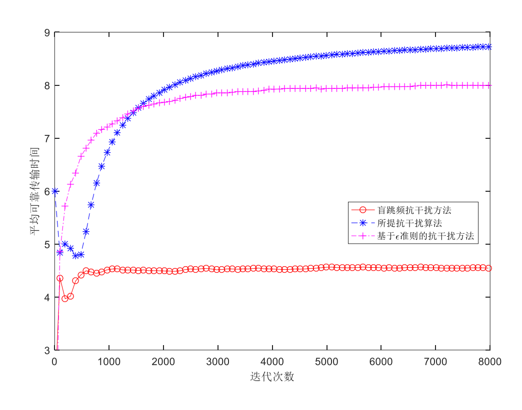


图 6　平均可靠传输时间性能比较

Fig .6 Comparison in the average reliable transmission time.

参考文献：

[1] 姚富强. 通信抗干扰工程与实践 [M]. 2 版. 北京: 电子工业出版社, 2012: 2-71. (Yao Fuqiang. Communication anti-jamming engineering and practice [M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2012: 2-71.)

[2] Kong Zhijie, Hao Xinhong, Li Ping, *et al.* Research on anti-frequency sweeping jamming method for frequency modulation fuze based on timing sequence and correlation detection [J]. Acta Armamentarii, 2017, 38 (8): 1483-1489.

[3] 陆丹丹. 跳频体制下的干扰检测及盲源分离 [D]. 成都: 电子科技大学, 2016: 16-21. (Lu Dandan. Interference detection and blind source separation technology in the frequency hopping system [D]. Chengdu: University of Electronic Science & Technology, 2016: 16-21.)

[4] Barbarossa S, Zanalda A. A combined wigner-ville and hough transform for cross-terms suppression and optimal detection and parameter estimation [C]// Proc. of Acoustics, Speech, and Signal Processing. 1992: 173-176.

[5] Barbarossa S. Analysis of multicomponent LFM signals by a combined wigner-hough ransform [J]. IEEE Trans on Signal Processing, 1995, 43 (6): 1511-1515.

[6] 夏彩杰, 王爱华, 安建平. 扫频干扰的自适应时变抑制研究 [J]. 计算机工程, 2008, 34 (4): 37-39. (Xia Caijie, Wang Aihua, An Jianping. Research on adaptive time-varying suppression of frequency sweeping interference [J]. Computer Engineering, 2008, 34 (4): 37-39.)

[7] 杨吉斌, 郑智, 张雄伟. 基于HMM的扩频通信扫频干扰抑制 [J]. 解放军理工大学学报: 自然科学版, 2004, 5 (4): 25-28. (Yang Jipin, Zheng Zhi, Zhang Xiongwei. Sweeping interference suppression based on the HMM in spread spectrum communication systems [J]. Journal of PLA University of Science & Technology: Natural Science Edition, 2004, 5 (4): 25-28.)

[8] 赵慧子, 孙克文. 基于分数阶傅里叶变换的GNSS接收机扫频干扰检测 [J]. 信息与电脑: 理论版, 2017 (1): 78-81. (Zhao Huizi, Sun Kewen. The sweep jamming detection for GNSS receiver based on fractional fourier transform [J]. China Computer & Communication, 2017 (1): 78-81.)

[9] 董彬虹, 杜洋, 周兰林, 等. 宽带扫频干扰下 FH//MFSK 系统性能分析 [J]. 电子科技大学学报, 2014, 43 (5): 659-662. (Dong Pinhong, Du Yang, Zhou Lanlin, *et al.* The performance analysis of the FH//MFSK system under the broadband sweep jamming [J]. Journal of Electronic Science and Technology, 2014, 43 (5): 659-662.)

[10] 吕再兴. 通信对抗中的干扰检测算法研究 [D]. 成都: 电子科技大学, 2011. (Lyu Zaixing. Research on jamming detection algorithm in communication countermeasures [D]. Chengdu: University of Electronic Science and Technology, 2011.)

[11] Ghorbel M B, Hamdaoui B, Guizani M, *et al.* Distributed learning-based cross-layer technique for energy-efficient multicarrier dynamic spectrum access with adaptive power allocation [J]. IEEE Trans on Wireless Communications, 2016, 15 (3): 1665-1674.

[12] Ali Ghaffari. Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms [J]. Wireless Networks, 2017, 23 (3): 703-714.

[13] Wang Beibei, Wu Yongle, Liu K. J R, *et al.* An anti-jamming stochastic game for cognitive radio networks [J]. IEEE Journal on Selected Areas in Communications, 2011, 29 (4): 877-889.

[14] Jia Luliang, Yao Fuqiang, Sun Youming, *et al.* A hierarchical learning solution for anti-jamming Stackelberg game with discrete power strategies [J]. IEEE Wireless Communications Letters, 2017, PP (99): 1-1.

[15] Sudharman K. Jayaweera. Signal processing for cognitive radios [M]. Wiley Publishing, 2014: 429-471.

[16] Wang Wenbo, Kwasinski Andres, Niyato Dusit, *et al.* A survey on applications of model-free strategy learning in cognitive wireless networks [J]. IEEE Communications Surveys & Tutorials, 2016, 18 (3): 1717-1757.